具有双向身份认证功能的量子密钥分发协议 *

郑　涛，张仕斌，李雪杨，熊金鑫，昌　燕

(成都信息工程大学 网络空间安全学院，成都 610225)

摘　要：提出了一种具有身份认证功能的量子密钥分发协议，该协议利用 Bell 态纠缠交换特性、Bell 基测量和按位异或运算，可以高效完成通信双方的身份认证；身份认证完成后，通信双方对手中粒子进行 Pauli 操作，能得到与对方拥有一样的 Bell 态粒子；通信双方按照约定的编码规则，得到相同二进制字符串作为密钥。分析表明，提出的密钥分发协议过程简单，操作容易实现，协议的安全性也能得到保证。

关键词：双向身份认证；纠缠交换；量子密钥分发

中图分类号：TP393.08　　doi: 10.19734/j.issn.1001-3695.2018.09.0750

Quantum key distribution protocol with two-way authentication

Zheng Tao, Zhang Shibin, Li Xueyang, Xiong Jinxin, Chang Yan

(*School of Cybersecurity*, *Chengdu University of Information Technology*, *Chengdu* 610225, *China*)

Abstract: This paper proposed a quantum key distribution protocol with identity authentication function, which utilized the Bell state entanglement switching feature, Bell-based measurement and bitwise XOR operation to efficiently complete identity authentication of both parties. After identity authentication was completed, communication was completed. The Pauli operation of the particles in both opponents could obtain the same Bell state particle as the other party; the communicating partied obtain the same binary string as the key according to the agreed encoding rules. The analysis shows that the key distribution protocol proposed in this paper is simple, easy to implement, and the security of the protocol can be guaranteed.

Key words: two-way authentication; entanglement swapping; quantum key distribution

0　引言

自第一个量子密钥分配(QKD)协议[1]被提出后，近年来量子密码学得到了巨大的发展。与经典密码学相比，量子密码学结合经典密码学和量子力学，利用量子效应实现了无条件安全的信息交互。为了满足社会对各种实际安全的需要，科研人员提出了大量的量子密码协议，主要包括量子密钥分配协议(QKD)[2~4]、量子直接安全通信[5~8](QSDC)、量子秘密共享[9,10](QSS)、量子数字签名及量子身份认证[11~14](QIA)等。QIA 是以量子态为载体，利用量子力学原理使得通信一方的身份被另一方确认。QKD 是通过量子信道，同时以经典信道作为辅助，给通信双方分配密钥。随着对量子技术研究的不断进步，在实际应用中量子隐私比较[15,16](QPC)、量子隐私数据库查询[17,18] (QPQ)等也在快速发展。量子通信是量子领域中最重要的应用之一，量子身份认证(QIA)是量子密钥分发(QKD)系统获取可靠密钥的前提，为通信双方的身份合法性提供重要依据。QIA 利用量子不可克隆及量子测不准原理对输入者个人信息进行处理并与系统中预先存储的个人信息进行比较，从而对个人身份进行肯定或者否定的判断。1999 年，Dusek 等人[13]首先提出利用经典信息认证算法对量子密钥系统经典消息进行认证的方案，从而达到抗干扰信道的效果。2000 年，曾贵华[19]利用量子的物理特性，提出了可信赖中心的 QIA，在此基础上进一步研究了无可信赖中心的量子身份认证方案，此方案采用认证密钥加密认证量子信息，以实现对认证方的动态认证，并且改进了认证的顺序，代替了经典公钥认证方案。到目前为止，QIA 共分为如下三类：第一类为点对点的 QIA，第二类是网络中的 QIA，第三类是 QIA 与 QKD 相结合。本文属于第三类的 QIA 方案。

本文提出了一个结合身份认证的量子密钥分配协议，通信参与者利用代表用户身份的二进制字符串进行 Bell 态的制备，双方对手中的粒子按照同一约定进行编码，随后进行粒子交换，完成 Bell 基测量以实现对 Bell 态粒子的纠缠交换，按编码规则对测量前后的粒子进行按位异或运算，就可以实现对通信双方的身份认证。待身份认证完成后，通信双方的任意一方进行 Pauli 门操作，可以使手中的粒子转换成和对方手中的粒子一样的 Bell 态粒子。按照同样的编码规则，通信双方可以获得一串相同二进制字符串，此时完成了密钥的分配。

1　准备知识

1.1　Bell 态纠缠交换

本协议用到的四种 Bell 态粒子可以表示为

收稿日期：2018-09-05；**修回日期：**2018-11-12　**基金项目：**国家重点研发计划资助项目(2017YFB0802302)；国家自然科学基金资助项目(61572086, 61402058)；四川省高校科研创新团队项目（17TD0009）；四川省学术和技术带头人培养支持经费资助项目（2016120080102643）；四川省应用基础项目(2017JY0168)；四川省重点研发计划项目（2018TJPT0012）；四川省科技支撑计划项目（2016FZ0112，2018GZ0204）

作者简介：郑涛（1994-），四川达州人，硕士研究生，主要研究方向为量子安全通信方面研究；张仕斌（1971-），男（通信作者），重庆丰都人，教授，博士，主要研究方向为网络安全、量子安全通信方面的研究（cuitzsb@cuit.edu.cn）；李雪杨（1995-），四川眉山人，硕士研究生，主要研究方向为量子安全通信研究；熊金鑫（1990-），男，河南信阳人，硕士研究生，主要研究方向为量子安全通信；昌燕（1979-），女（蒙古族），内蒙古人，副教授，博士，主要研究方向为量子密码、信息安全.

$$|\phi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|00\rangle\pm|11\rangle),|\psi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|01\rangle\pm|10\rangle) \tag{1}$$

两个 Bell 态粒子若处于 $|\phi^{+}\rangle$ 态，对它们进行 Bell 态纠缠交换，则有下面等式成立：

$$\begin{aligned}|\phi^{+}>_{12}|\phi^{+}>_{34}&=\frac{1}{\sqrt{2}}(|00\rangle+|00\rangle)_{12}\otimes\frac{1}{\sqrt{2}}(|00\rangle+|00\rangle)_{34}\\&=\frac{1}{\sqrt{2}}\begin{pmatrix}|\phi^{+}>_{13}|\phi^{+}>_{24}+|\phi^{-}>_{13}|\phi^{-}>_{24}\\+|\psi^{+}>_{13}|\psi^{+}>_{24}+|\psi^{-}>_{13}|\psi^{-}>_{24}\end{pmatrix}\end{aligned} \tag{2}$$

如果对 1、3 粒子进行 Bell 基测量，2、4 粒子则会纠缠到对应的状态。例如，对 1、3 粒子测量的结果为 $|\psi^{+}\rangle_{13}$ ，2、4 粒子的状态为 $|\psi^{+}\rangle_{24}$ 。若不考虑其相位问题，任意两个 Bell 态的纠缠情况如表 1 所示。

表 1　任意两个 Bell 态的纠缠交换

Table 1　Entanglement swapping of arbitrary two Bell States

$\|\phi^{+}\rangle_{12}$	$\|\phi^{+}\rangle_{34}$	$\|\phi^{+}\rangle_{13}\|\phi^{+}\rangle_{24},\|\phi^{-}\rangle_{13}\|\phi^{-}\rangle_{24}$, $\|\psi^{+}\rangle_{13}\|\psi^{+}\rangle_{24},\|\psi^{-}\rangle_{13}\|\psi^{-}\rangle_{24}$
$\|\phi^{+}\rangle_{12}$	$\|\phi^{-}\rangle_{34}$	$\|\phi^{+}\rangle_{13}\|\phi^{-}\rangle_{24},\|\phi^{-}\rangle_{13}\|\phi^{+}\rangle_{24}$, $\|\psi^{+}\rangle_{13}\|\psi^{-}\rangle_{24},\|\psi^{-}\rangle_{13}\|\psi^{+}\rangle_{24}$
$\|\phi^{+}\rangle_{12}$	$\|\psi^{+}\rangle_{34}$	$\|\phi^{+}\rangle_{13}\|\psi^{+}\rangle_{24},\|\psi^{+}\rangle_{13}\|\phi^{+}\rangle_{24}$, $\|\phi^{-}\rangle_{13}\|\psi^{-}\rangle_{24},\|\psi^{-}\rangle_{13}\|\phi^{-}\rangle_{24}$
$\|\phi^{+}\rangle_{12}$	$\|\psi^{-}\rangle_{34}$	$\|\phi^{+}\rangle_{13}\|\psi^{-}\rangle_{24},\|\psi^{-}\rangle_{13}\|\phi^{+}\rangle_{24}$, $\|\phi^{-}\rangle_{13}\|\psi^{+}\rangle_{24},\|\psi^{+}\rangle_{13}\|\phi^{-}\rangle_{24}$
$\|\phi^{-}\rangle_{12}$	$\|\phi^{+}\rangle_{34}$	$\|\phi^{-}\rangle_{13}\|\phi^{+}\rangle_{24},\|\phi^{+}\rangle_{13}\|\phi^{-}\rangle_{24}$, $\|\psi^{+}\rangle_{13}\|\psi^{-}\rangle_{24},\|\psi^{-}\rangle_{13}\|\psi^{+}\rangle_{24}$
$\|\phi^{-}\rangle_{12}$	$\|\phi^{-}\rangle_{34}$	$\|\phi^{-}\rangle_{13}\|\phi^{-}\rangle_{24},\|\phi^{+}\rangle_{13}\|\phi^{+}\rangle_{24}$, $\|\psi^{+}\rangle_{13}\|\psi^{+}\rangle_{24},\|\psi^{-}\rangle_{13}\|\psi^{-}\rangle_{24}$
$\|\phi^{-}\rangle_{12}$	$\|\psi^{+}\rangle_{34}$	$\|\phi^{-}\rangle_{13}\|\psi^{+}\rangle_{24},\|\psi^{+}\rangle_{13}\|\phi^{-}\rangle_{24}$, $\|\phi^{+}\rangle_{13}\|\psi^{-}\rangle_{24},\|\psi^{-}\rangle_{13}\|\phi^{+}\rangle_{24}$
$\|\phi^{-}\rangle_{12}$	$\|\psi^{-}\rangle_{34}$	$\|\phi^{-}\rangle_{13}\|\psi^{-}\rangle_{24},\|\psi^{-}\rangle_{13}\|\phi^{-}\rangle_{24}$, $\|\phi^{+}\rangle_{13}\|\psi^{+}\rangle_{24},\|\psi^{+}\rangle_{13}\|\phi^{+}\rangle_{24}$
$\|\psi^{+}\rangle_{12}$	$\|\phi^{+}\rangle_{34}$	$\|\psi^{+}\rangle_{13}\|\phi^{+}\rangle_{24},\|\phi^{+}\rangle_{13}\|\psi^{+}\rangle_{24}$, $\|\phi^{-}\rangle_{13}\|\psi^{-}\rangle_{24},\|\psi^{-}\rangle_{13}\|\phi^{-}\rangle_{24}$
$\|\psi^{+}\rangle_{12}$	$\|\phi^{-}\rangle_{34}$	$\|\psi^{+}\rangle_{13}\|\phi^{-}\rangle_{24},\|\phi^{-}\rangle_{13}\|\psi^{+}\rangle_{24}$, $\|\phi^{+}\rangle_{13}\|\psi^{-}\rangle_{24},\|\psi^{-}\rangle_{13}\|\phi^{+}\rangle_{24}$
$\|\psi^{+}\rangle_{12}$	$\|\psi^{+}\rangle_{34}$	$\|\psi^{+}\rangle_{13}\|\psi^{+}\rangle_{24},\|\psi^{-}\rangle_{13}\|\psi^{-}\rangle_{24}$, $\|\phi^{-}\rangle_{13}\|\phi^{-}\rangle_{24},\|\phi^{+}\rangle_{13}\|\phi^{+}\rangle_{24}$
$\|\psi^{+}\rangle_{12}$	$\|\psi^{-}\rangle_{34}$	$\|\psi^{+}\rangle_{13}\|\psi^{-}\rangle_{24},\|\psi^{-}\rangle_{13}\|\psi^{+}\rangle_{24}$, $\|\phi^{+}\rangle_{13}\|\phi^{-}\rangle_{24},\|\phi^{-}\rangle_{13}\|\phi^{+}\rangle_{24}$
$\|\psi^{-}\rangle_{12}$	$\|\phi^{+}\rangle_{34}$	$\|\phi^{-}\rangle_{13}\|\phi^{+}\rangle_{24},\|\phi^{+}\rangle_{13}\|\psi^{-}\rangle_{24}$, $\|\phi^{-}\rangle_{13}\|\psi^{+}\rangle_{24},\|\psi^{+}\rangle_{13}\|\phi^{-}\rangle_{24}$
$\|\psi^{-}\rangle_{12}$	$\|\phi^{-}\rangle_{34}$	$\|\psi^{-}\rangle_{13}\|\phi^{-}\rangle_{24},\|\phi^{-}\rangle_{13}\|\psi^{-}\rangle_{24}$, $\|\phi^{+}\rangle_{13}\|\psi^{+}\rangle_{24},\|\psi^{+}\rangle_{13}\|\phi^{+}\rangle_{24}$
$\|\psi^{-}\rangle_{12}$	$\|\psi^{+}\rangle_{34}$	$\|\psi^{-}\rangle_{13}\|\psi^{+}\rangle_{24},\|\psi^{+}\rangle_{13}\|\psi^{-}\rangle_{24}$, $\|\phi^{+}\rangle_{13}\|\phi^{-}\rangle_{24},\|\phi^{-}\rangle_{13}\|\phi^{+}\rangle_{24}$
$\|\psi^{-}\rangle_{12}$	$\|\psi^{-}\rangle_{34}$	$\|\psi^{-}\rangle_{13}\|\psi^{-}\rangle_{24},\|\psi^{+}\rangle_{13}\|\psi^{+}\rangle_{24}$, $\|\phi^{+}\rangle_{13}\|\phi^{+}\rangle_{24},\|\phi^{-}\rangle_{13}\|\phi^{-}\rangle_{24}$

若约定用 00 表 示 $|\phi^{+}\rangle$ 态，01 表示 $|\phi^{-}\rangle$ 态，10 表示 $|\psi^{+}\rangle$ 态，11 表示 $|\psi^{-}\rangle$ 态，且假设纠缠交换前的两个 Bell 态粒子的二进制表示为 P_{12} 和 P_{34}，纠缠交换后的两个 Bell 态粒子的二进制表示为 P_{13} 和 P_{24} 。若两个 Bell 态粒子均处于 $|\phi^{+}\rangle$ 态，则纠缠交换后的两个 Bell 态粒子以 $\frac{1}{4}$ 的概率处于 $|\phi^{+}>_{13}|\phi^{+}>_{24}$，以 $\frac{1}{4}$ 的概率处于 $|\phi^{-}>_{13}|\phi^{-}>_{24}$，以 $\frac{1}{4}$ 的概率处于 $|\psi^{+}>_{13}|\psi^{+}>_{24}$，以 $\frac{1}{4}$ 的概率处于 $|\psi^{-}>_{13}|\psi^{-}>_{24}$。如果纠缠交换后两个 Bell 态粒子处于 $|\phi^{+}>_{13}|\phi^{+}>_{24}$，则有 $P_{12}\oplus P_{34}=P_{13}\oplus P_{24}$=00⊕00=00 。如果纠缠交换后两个 Bell 态粒子处于 $|\phi^{-}>_{13}|\phi^{-}>_{24}$ ，则有 $P_{12}\oplus P_{34}=P_{13}\oplus P_{24}$=01⊕01=00 。如果纠缠交换后两个 Bell 态粒子处于 $|\psi^{-}>_{13}|\psi^{-}>_{24}$，则有 $P_{12}\oplus P_{34}=P_{13}\oplus P_{24}$=11⊕11=00 。如果纠缠交换后两个 Bell 态粒子处于 $|\psi^{+}>_{13}|\psi^{+}>_{24}$ ，则有 $P_{12}\oplus P_{34}=P_{13}\oplus P_{24}$=10⊕10=00 。经过推导发现，任意两种 bell 态纠缠交换后，都满足式（3）。

$$P_{12}\oplus P_{34}=P_{13}\oplus P_{24} \tag{3}$$

且任意两种 bell 态纠缠交换对应的二进制关系如表 2 所示。

表 2　两个 bell 态纠缠交换二进制表示关系

Table 2　The binary representation relation of two Bell states entanglement swapping

P_{12}	P_{34}	纠缠交换后 $P_{13}\oplus P_{24}$
00	00	00⊕00=00， 01⊕01=00， 10⊕10=00， 11⊕11=00
00	01	00⊕01=01， 01⊕00=01， 10⊕11=01， 11⊕10=01
00	10	00⊕10=10， 10⊕00=10， 01⊕11=10， 11⊕01=10
00	11	00⊕11=11， 11⊕00=11， 01⊕10=11， 10⊕01=11
01	00	01⊕00=01， 00⊕01=01， 10⊕11=01， 11⊕10=01
01	01	01⊕01=00， 00⊕00=00， 10⊕10=00， 11⊕11=00
01	10	01⊕10=11， 10⊕01=11， 00⊕11=11， 11⊕00=11
01	11	01⊕11=10， 11⊕01=10， 00⊕10=10， 10⊕00=10
10	00	10⊕00=10， 00⊕10=10， 01⊕11=10， 11⊕01=10
10	01	10⊕01=11， 01⊕10=11， 00⊕11=11， 11⊕00=11
10	10	10⊕10=00， 00⊕00=00， 01⊕01=00， 10⊕10=00
10	11	10⊕11=01， 11⊕10=01， 00⊕01=01， 01⊕00=01
11	00	11⊕00=11， 00⊕11=11， 01⊕10=11， 10⊕01=11
11	01	11⊕01=10， 01⊕11=10， 00⊕10=10， 10⊕00=10
11	10	11⊕10=01， 10⊕11=01， 01⊕00=01， 00⊕01=01
11	11	11⊕11=00， 10⊕10=00， 00⊕00=00， 01⊕01=00

1.2　Pauli 矩阵变换

Pauli 矩阵可以表示如下：

$$X=\begin{pmatrix}0&1\\1&0\end{pmatrix}\ Y=\begin{pmatrix}0&-i\\i&0\end{pmatrix}$$
$$Z=\begin{pmatrix}1&0\\0&-1\end{pmatrix}\ I=\begin{pmatrix}1&0\\0&1\end{pmatrix} \tag{4}$$

其中：X 和 Z 分别称为比特翻转和相位翻转操作符。如果对一个量子比特进行 X 操作，有 $X|0\rangle=|1\rangle$ ， $X|1\rangle=|0\rangle$ 。对其进行 Z 操作，有 $Z|+\rangle=|-\rangle$， $Z|-\rangle=|+\rangle$ 。对其进行 iY 操作，同时产生比特翻转和相位翻转效果。

$$iY=ZX=\begin{pmatrix}1&0\\0&-1\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}=\begin{pmatrix}0&1\\-1&0\end{pmatrix}=i\begin{pmatrix}0&-i\\i&0\end{pmatrix} \tag{5}$$

四个 Bell 态粒子状态经过 Pauli 矩阵转换结果如表 3 所示。

表 3　四种 Bell 态粒子经过 Pauli 矩阵转换结果

Table 3. Results of transformation of four Bell state particles through Pauli matrix

Bell 态	$\|\phi^+\rangle$	$\|\phi^-\rangle$	$\|\psi^+\rangle$	$\|\psi^-\rangle$
$\|\phi^+\rangle$	I	σ_z	σ_x	$i\sigma_y$
$\|\phi^-\rangle$	σ_z	I	$i\sigma_y$	σ_x
$\|\psi^+\rangle$	σ_x	$i\sigma_y$	I	σ_z
$\|\psi^-\rangle$	$i\sigma_y$	σ_x	σ_z	I

2　协议描述

a）Alice 的二进制身份字符串为 $ID_A=\{P^1{}_{12}, P^2{}_{12} \ldots P^{2n}{}_{12}\}$，Bob 的二进制身份字符串为 $ID_B=\{P^1{}_{34}, P^2{}_{34} \ldots P^{2n}{}_{34}\}$。Alice 和 Bob 秘密共享 ID_A 和 ID_B。Alice 根据 ID_A 制备 Bell 态粒子序列 S_{ID_A}，Bob 根据 ID_B 制备 Bell 态粒子序列 S_{ID_B}。双方约定制备规则为：如果身份字符串的当前位是 00，则制备的粒子态处于 $|\phi>^+$。如果身份字符串的当前位是 01，则制备的粒子态处于 $|\phi>^-$ 如果身份字符串的当前位是 10，则制备的粒子态处于 $|\psi>^+$。如果身份字符串的当前位是 11，则制备的粒子态处于 $|\psi>^-$。

b）Alice 抽取所有 S_{ID_A} 粒子序列的第二个粒子，并随机插入足量的 Bell 态粒子作为诱骗粒子，记录其位置信息后 Alice 将这段粒子序列 S'_{ID_A}，发送给 Bob，Bob 抽取所有 S_{ID_B} 粒子序列的第一个粒子，插入足量的处于 Bell 态的诱骗粒子，并记录位置信息后记为 S'_{ID_B}，发送给 Alice。双方同样按照约定的编码规则，对诱骗粒子进行编码：$|\phi^+\rangle$ 编码为 00，$|\phi^-\rangle$ 编码为 01，$|\psi^+\rangle$ 编码为 10，$|\psi^-\rangle$ 编码为 11。

c）双方都接收到粒子序列 S'_{ID_A} 和 S'_{ID_B} 后，公布诱骗粒子的位置和诱骗粒子的二进制编码字符串。各自抽取出诱骗粒子后进行测量，并比较误码率。若误码率高于规定的阈值，协议终止。

d）完成误码率检测后，双方对手中的粒子进行 Bell 基测量，测量的结果按如下规则编码：$|\phi^+\rangle$ 编码为 00，$|\phi^-\rangle$ 编码为 01，$|\psi^+\rangle$ 编码为 10，$|\psi^-\rangle$ 编码为 11。得到 ID_A' 和 ID_B'，此时完成纠缠交换。双方公布 ID_A' 和 ID_B'，各自判断 $ID_A \oplus ID_B = ID_A' \oplus ID_B'$ 是否成立，根据式(2)，若成立，则完成对通信另一方的身份认证。

e）完成身份认证后，Alice 根据 ID_B' 和纠缠交换的性质，由表 1 可以推出 Bob 手中 Bell 态序列的信息。根据表 3 所示的 Pauli 操作，Alice 将手中的粒子执行相应的操作，即可得到与 Bob 相同的粒子序列。双方按照 1)的编码规则对得到的粒子序列进行编码，可以得到相同的二进制字符串作为密钥序列。

3　协议举例

a）假设 Alice 的二进制身份字符串 $ID_A=11010100$，Bob 的二进制身份字符串 $ID_B=10011100$。Alice 和 Bob 共享 ID_A 和 ID_B。Alice 根据 ID_A 制备粒子序列 $S_{ID_A}=\{|\psi^-\rangle,|\phi^-\rangle,|\phi^-\rangle,|\phi^+\rangle\}$，Bob 根据 ID_B 制备粒子序列为 $S_{ID_B}=\{|\psi^+\rangle,|\phi^-\rangle,|\psi^-\rangle,|\phi^+\rangle\}$。制备规则为：如果身份字符串当前位为 00 制备处于 $|\phi^+\rangle$ 态的粒子，当前位为 01 制备处于 $|\phi^-\rangle$ 态的粒子，当前位为 10 制备处于 $|\psi^+\rangle$ 态的粒子，当前位为 11 制备处于 $|\psi^-\rangle$ 态的粒子。

b）Alice 抽取所有 S_{ID_A} 粒子序列的第二个粒子，并随机插入足量的 Bell 态粒子作为诱骗粒子，记录其位置信息后 Alice 将这段粒子序列 S'_{ID_A}，发送给 Bob，Bob 抽取所有 S_{ID_B} 粒子序列的第一个粒子，插入足量的处于 Bell 态的诱骗粒子，并记录位置信息后记为 S'_{ID_B}，发送给 Alice。双方同样按照约定的编码规则，对诱骗粒子进行编码：$|\phi^+\rangle$ 编码为 00，$|\phi^-\rangle$ 编码为 01，$|\psi^+\rangle$ 编码为 10，$|\psi^-\rangle$ 编码为 11。假设 S'_{ID_A} 中诱骗粒子位置信息为 $L_A=\{2,3,5,7\}$，L_A 表示诱骗粒子在 S'_{ID_A} 序列中的第 2,3,5,7 位。状态信息为 $\{|\psi^-\rangle,|\phi^-\rangle,|\phi^+\rangle,|\psi^+\rangle\}$，编码为 $E_A=\{11,01,00,10\}$。$L_B=\{1,3,4,6\}$ 表示诱骗粒子在 S'_{ID_B} 序列中的第 1,3,4,6 位。状态信息为 $\{|\phi^+\rangle,|\psi^-\rangle,|\phi^-\rangle,|\phi^+\rangle\}$，编码为 $E_B=\{00,11,01,00\}$。

c）双方都接收到粒子序列 S'_{ID_A} 和 S'_{ID_B} 后，公布诱骗粒子的位置和诱骗粒子的二进制编码字符串。各自抽取出诱骗粒子后进行测量，并比较误码率。若误码率高于规定的阈值，协议终止。

d）完成误码率检测后，双方对手中的粒子进行 Bell 基测量，此时 Alice 手中的粒子序列为 $New_{ID_A}=\{|\psi^+\rangle,|\phi^+\rangle,|\psi^-\rangle,|\phi^-\rangle\}$，Bob 手中的粒子序列为 $New_{ID_B}=\{|\psi^-\rangle,|\phi^+\rangle,|\phi^-\rangle,|\phi^-\rangle\}$。按如下规则编码：$|\phi^+\rangle$ 编码为 00，$|\phi^-\rangle$ 编码为 01，$|\psi^+\rangle$ 编码为 10，$|\psi^-\rangle$ 编码为 11。得到 $ID_A'=\{10,00,11,01\}$ 和 $ID_B'=\{11,00,01,01\}$，此时完成纠缠交换。双方公布 ID_A' 和 ID_B'，根据公式 $ID_A \oplus ID_B = ID_A' \oplus ID_B'$，因为

$$ID_A \oplus ID_B = 11010100 \oplus 10011100 = 01001000$$

$$ID_A' \oplus ID_B' = 10001101 \oplus 11000101 = 01001000$$

所以该公式满足，证明通信双方的身份合法。

e)此时 Alice 手中的粒子序列为 $\{|\psi^+\rangle,|\phi^+\rangle,|\psi^-\rangle,|\phi^-\rangle\}$，Bob 手中的粒子序列为 $\{|\psi^-\rangle,|\phi^+\rangle,|\phi^-\rangle,|\phi^-\rangle\}$。根据表 1 和 3，Alice 对手中的粒子进行 Pauli 操作的顺序为 $\{\sigma_z, I, \sigma_x, I\}$，此时 Alice 手中的粒子状态变为 $\{|\psi^-\rangle,|\phi^+\rangle,|\phi^-\rangle,|\phi^-\rangle\}$，按照 a）中的编码规则，双方得到相同的二进制字符串 $key=11000101$。此时完成了密钥分配。身份认证和密钥分配过程如图 1 所示。

4　安全性分析

根据协议步骤可知，当身份认证完成后，密钥分配的过程不会有安全隐患。所以本协议的安全性分析主要分析身份认证过程。

4.1　冒充攻击

假设 Alice 被 Eve 冒充，Bob 是合法的。Eve 在不知道 ID_A 的情况下和 Bob 通信。Eve 随机制备 Bell 态粒子序列 S_{ID_E}，并发送所有 S_{ID_E} 的第一个粒子给 Bob，Bob 发送所有 S_{ID_B} 的第一个粒子给 Eve。接收完成后，Eve 拥有的粒子序列记为 S'_{ID_E}，Bob 拥有的粒子序列记为 S'_{ID_B}。Eve 和 Bob 对手中的粒子进行 Bell 基测量，完成纠缠交换。Eve 对测量后的粒子状态用约定的编码方式编码成二进制字符串，记为 ID'_E，Bob 手中的粒子也经过同样的操作后，记为 ID'_B。当 Bob 对 Alice 进行身份认证时，Eve 公布 ID'_E，根据式(2)，由于 $ID_A \oplus ID_B \neq ID'_E \oplus ID'_B$，Eve 不能通过身份认证。同理，Eve 冒充 Bob 也不能通过身份认证。

4.2　截获/重发攻击和中间人攻击

假设 Eve 截获 Alice 发送给 Bob 的粒子序列 S'_{ID_A}，由于此时 Bob 没有接收到 Alice 发来的粒子序列，Alice 不会宣布在 S'_{ID_A} 序列中诱骗粒子的二进制字符串和位置信息。Eve 不论采取什么手段对 S'_{ID_A} 进行测量，当 Eve 测量完成并发给 Bob 后，都会使得 Bob 对诱骗粒子测量得到的结果与 Alice 公布的状态完全不同。执行窃听检测时，Eve 会被 Bob 发现。协议随即终止。假设由于疏忽或其他原因 Alice 公布了 S'_{ID_A} 中诱骗粒子的二进制字符串和位置信息，由于 Eve 无法得知通信双方约定的对诱骗粒子的编码规则，Eve 仍旧无法正确的对诱骗粒子进行正确的测量，从而导致通信双方的窃听检测不通过。

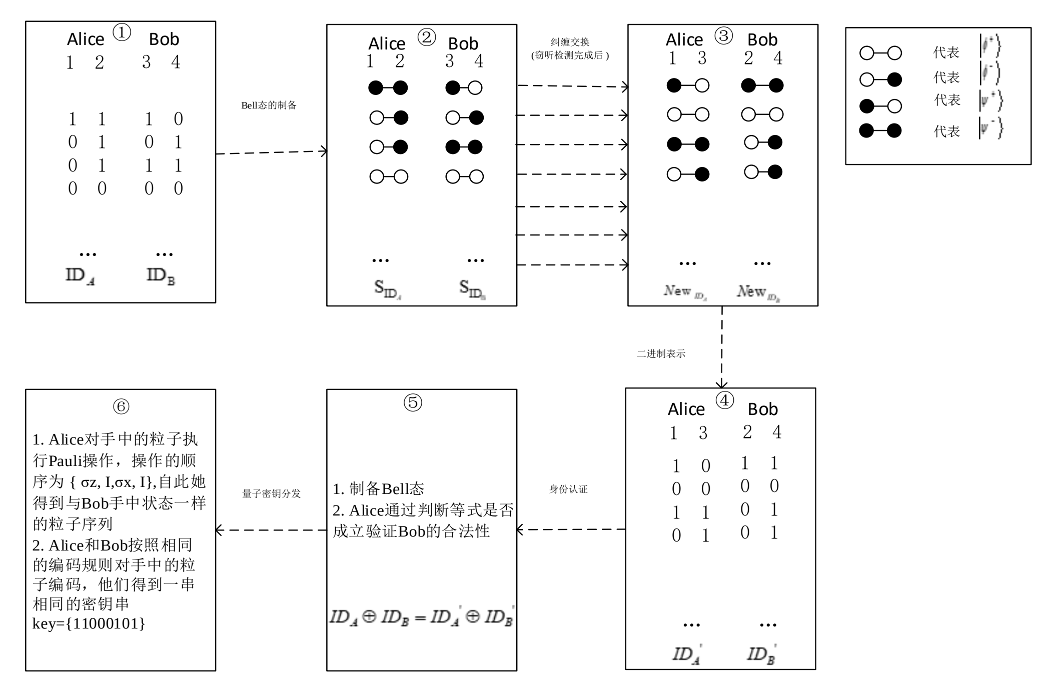


图 1　身份认证和密钥分配过程

Fig. 1　Identity authentication and key distribution process

4.3　ID_A 和 ID_B 的安全性

由于 ID_A 和 ID_B 是双方在开始通信之前秘密共享的，非法用户无法得知 ID_A 和 ID_B 。如果 Eve 采取穷举法猜测 ID_A 和，当 ID_A 和 ID_B 的长度为 2n 时，Eve 能正确猜出的概率 ID_B 为 $\frac{1}{4^n}$ 。当 ID_A 和 ID_B 的长度足够长时，Eve 能猜出的概率趋近于零。如果 Eve 采取截获/重发攻击来得到 ID_A 和 ID_B，Eve 截取 Alice 发送给 Bob 的粒子序列 S_{ID_A}，由于 Eve 的测量无法推测 Alice 手中粒子序列的详情，且会导致 Alice 手中粒子的塌缩。使得通信双方无法完成纠缠交换，进而无法通过式（2），身份认证无法通过。如果 Eve 试图通过通信双方公布的 ID_A' 和 ID_B' 来猜测 ID_A 和 ID_B， 由于 ID_A' 和 ID_B' 是两个 Bell 态粒子纠缠交换后四个混合态的二进制表示，所以 ID_A' 和 ID_B' 都以 $p=\frac{1}{4}$ 的概率处于 $\{00,01,10,11\}$，Eve 无法得到 ID_A 和 ID_B 的有效信息。故 ID_A' 和 ID_B' 的公布不会导致 ID_A 和 ID_B 的泄露。且 ID_A 和 ID_B 是可以重复利用的。

5　性能分析

首先分析身份认证过程，在已有的身份认证协议中，大部分协议都是抽取用于通信的粒子进行窃听检测，这种方法在一定程度上减小了协议认证复杂性，但是对于身份认证过程，由于有相当一部分粒子用于窃听检测，导致身份认证的效率下降。在本协议中，由于通信双方按照各自公开的 ID 进行 Bell 态粒子制备，完成粒子制备后，双方均对粒子序列插入额外的窃听粒子，且窃听粒子的二进制编码信息与 ID 编码信息一致，在同样减小了协议的复杂度基础上，较好了提高了用于身份认证的粒子使用效率。

分析密钥生成效率，根据协议描述，Alice 与 Bob 完成身份认证（QIA）后，双方根据公开的 ID'信息，结合简单的 Pauli 门操作，就可以得到与对方手中相同的粒子序列。经过粒子编码后，Alice 和 Bob 得到相同二进制密钥串。由于本协议在 QKD 步骤前，已经完成了对通信参与双方对身份认证，此时 Alice 和 Bob 都是合法的参与者，故他们不再对手中的粒子进一步的进行窃听检测等容易造成粒子损失的操作，这即是说，QIA 完成后，双方手中的全部粒子都将用作密钥建立过程。与经典的 BB84、B92 等协议做对比，本协议有较好的密钥生成效率。

如安全性分析部分描述的，本协议的安全性分析主要聚焦在身份认证过程中。结合经典的非对称加密思想，本协议提出通信双方用公开的 ID 进行粒子的制备，身份的验证等步骤。通信双方在发送的粒子序列中插入了足量的窃听检测粒子，这使得本协议能抵抗绝大部分的攻击策略，使得本协议有较好的安全性能来满足身份认证和密钥建立两个过程。

6　结束语

本文提出了一种基于 Bell 态粒子纠缠交换特性的具有身份认证功能的量子密钥分发协议。通信双方只需按照代表

自身身份的二进制字符串制备 Bell 态序列，然后 Alice 抽取她手中所有 Bell 态的第一个粒子，插入足量的诱骗粒子后发送给 Bob，Bob 也对手中的粒子做同样的操作。双方均完成粒子接收后，对各自手中的粒子做 Bell 基测量，并将测量结果进行二进制表示。双方公布测量结果对应的二进制就可以完成对对方的身份认证。完成身份认证后，通信的发起方对手中粒子做相应的 Pauli 操作，得到与另一个通信方相同的 Bell 态粒子。通信双方按照相同的编码规则对手中的粒子进行二进制编码，可以使得双方拥有相同的密钥串。对本协议的安全性分析表明，只要代表通信双方身份信息的二进制字符串没有泄露，本协议就可以抵御冒充攻击和截获/重发与中间人攻击，身份认证过程就是真实有效的。在实际的应用中，本协议的实现只取决于 Bell 态的精确制备、Bell 态的精确测量操作和 Pauli 门的正确实现。且代表用户身份的二进制字符串可以重复利用，ID_A 和 ID_B 的安全性也得到了保证。

参考文献：

[1] Bennett C H, Brassard G. Quantum cryptography:public key distribution and coin tossing [C]// Proc of IEEE International Conference on Computers Systems and Signal Processing. 1984: 175-179.

[2] Bennett C H. Quantum cryptography using any two nonorthogonal

states. [J]. Physical Review Letters, 1992, 68 (68): 3121-3124.

[3] Wang Chao, Wang Shuang, Yin Zhenqian, *et al.* Experimental measurement-device-independent quantum key distribution with uncharacterized encoding [J]. Optics Letters, 2016, 41 (23): 5596-5599.

[4] Curty M, Xu Feihu, Cui Wei, *et al.* Finite-key analysis for measurement-device-independent quantum key distribution [J]. Nature Communications, 2014, 5 (4): 643-648.

[5] Patwardhan S, Moulick S R, Panigrahi P K. Efficient controlled quantum secure direct communication protocols [J]. International Journal of Theoretical Physics, 2016, 55 (7): 3280-3288.

[6] Patwardhan S, Moulick S R, Panigrahi P K. Efficient controlled quantum secure direct communication protocols [J]. International Journal of Theoretical Physics, 2016, 55 (7): 3280-3288.

[7] Chang Yan, Xu Chunxiang, Zhang Shibin, *et al.* Quantum secure direct communication and authentication protocol with single photons [J]. Chinese Science Bulletin, 2013, 58 (36): 4571-4576.

[8] Cai Qingyu, Li Baiwen. Deterministic secure communication without using entanglement [J]. Chin Phys Lett, 2004, 21 (4): 601-603.

[9] Qin Huawang, Dai Yuewei. Verifiable (t, n) threshold quantum secret sharing using d-dimensional Bell state [J]. Information Processing Letters, 2016, 116 (5): 351-355.

[10] Mishra S, Shukla C, Pathak A, *et al.* An integrated hierarchical dynamic quantum secret sharing protocol [J]. International Journal of Theoretical Physics, 2015, 54 (9): 1-12.

[11] Wang Ding, He Debiao, Wang Ping, *et al.* Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment [J]. IEEE Trans on Dependable and Secure Computing, 2015, 12 (4): 428-442.

[12] Wang Ding, Wang Ping. Two birds with one stone: two-factor authentication with security beyond conventional bound [J]. IEEE Trans on Dependable and Secure Computing, 2018, 15(4): 708-722.

[13] DuŠek M, Haderka O, Hendrych M, *et al.* Quantum identification system[J]. Physical Review A, 1999, 60(1): 149-156.

[14] Yuan Hao, Liu Yimin, Pan Guozhu, *et al.* Quantum identity authentication based on ping-pong technique without entanglements [J]. Quantum Information Processing, 2014, 13 (11): 2535-2549.

[15] Gao Gan. Secure multiparty quantum secret sharing with the collective eavesdropping-check character [J]. Quantum Information Processing, 2013, 12 (1): 55-68.

[16] Wang Yukun, Zhang Jie, Huang Wei, *et al.* A quantum private comparison protocol with splitting information carriers [J]. International Journal of Theoretical Physics, 2015, 54 (1): 281-291.

[17] Wei Chunyan, Wang Tianyin, Gao Fei. Practical quantum private query with better performance in resisting joint-measurement attack [J]. Physical Review A, 2016, 93 (4) .

[18] Gao Fei, Liu Bin, Huang Wei, *et al.* Postprocessing of the Oblivious Key in Quantum Private Query [J]. IEEE Journal of Selected Topics in Quantum Electronics, 2014, 21 (3): 98-108.

[19] 曾贵华. 不依赖第三方的动态量子身份认证方案 [J]. 电子学报, 2004, 32 (7): 1148-1152. (Zeng Guihua. Dynamic quantum identity authentication scheme independent of the third party [J]. Acta electronica Sinica, 2004, 32 (7): 1148-1152.)